

Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of Claims:

Claim 1 (currently amended): A computer system comprising a memory portion ~~configured to store~~ containing an encrypted data file and an operating system comprising a kernel, the kernel configured to decrypt an encrypted directory entry to determine a location of the encrypted data file and to decrypt the encrypted data file to access data contained therein ~~encrypt and decrypt the data accessed using an encrypted directory and transferred between the memory portion and a secondary device.~~

Claim 2 (currently amended): The computer system of claim 1, wherein the kernel comprises an encryption engine configured to encrypt clear data files to generate cipher data files, the encryption engine further configured to decrypt the cipher data files to generate the clear data files.

Claim 3 (currently amended): The computer system of claim 2, wherein the memory portion is coupled to the encryption engine and configured to store the cipher data files.

Claim 4 (currently amended): The computer system of claim 2, wherein the encryption engine is configured to encrypt the clear data files and decrypt the cipher data files according to a symmetric key encryption algorithm.

Claim 5 (previously presented): The computer system of claim 4, wherein the symmetric key encryption algorithm is based on a block cipher.

Claim 6 (previously presented): The computer system of claim 5, wherein the symmetric key encryption algorithm comprises Rijndael algorithm.

Claim 7 (previously presented): The computer system of claim 6, wherein the symmetric key encryption algorithm uses a block size of 128 bits, 192 bits, 256 bits, 512 bits, 1024 bits, or 2048 bits.

Claim 8 (previously presented): The computer system of claim 6, wherein the symmetric key encryption algorithm uses a key length of 128 bits, 192 bits, 256 bits, 512 bits, 1024 bits, or 2048 bits.

Claim 9 (previously presented): The computer system of claim 5, wherein the symmetric key encryption algorithm comprises a DES algorithm.

Claim 10 (previously presented): The computer system of claim 5, wherein the symmetric key encryption algorithm comprises a Triple-DES algorithm.

Claim 11 (previously presented): The computer system of claim 5, wherein the symmetric key encryption algorithm comprises an algorithm selected from the group consisting of IDEA, Blowfish, Twofish, and CAST-128.

Claim 12 (previously presented): The computer system of claim 1, wherein the kernel comprises a UNIX operating system.

Claim 13 (previously presented): The computer system of claim 12, wherein the UNIX operating system is a System V-Revision.

Claim 14 (currently amended): The computer system of claim 1, wherein the memory portion comprises a first logical protected memory configured to store encrypted [[file]] data files and a second logical protected memory configured to store encrypted key data.

Claim 15 (currently amended): The computer system of claim 14, further comprising an encryption key management system, the encryption key management system configured to control access to the encrypted [[file]] data files and the encrypted key data.

Claim 16 (currently amended): The computer system of claim 15, wherein the encryption key management system comprises a key engine, the key engine configured to receive a pass key and ~~[[the]]~~ a data file name to generate an encrypted data file name key, the key engine further configured to use the encrypted data file name key and data file contents to generate an encrypted data file contents key, the key engine further configured to encrypt the data file contents with the encrypted data file contents key to generate encrypted data file contents and to encrypt the data file name with the encrypted data file name key to generate an encrypted data file name.

Claim 17 (currently amended): The computer system of claim 16, wherein the encryption key management system is configured to store ~~the~~ encrypted data file ~~names~~ name, wherein the data file ~~names~~ are name is associated with the encrypted file contents.

Claim 18 (currently amended): The computer system of claim 17, wherein the encryption key management system is further configured to grant access to a data file if a corresponding access permission of the data file is a predetermined value.

Claim 19 (currently amended): The computer system of claim 1, further comprising a secondary device coupled to the memory, wherein the secondary device stores the encrypted data file and is accessed using a file abstraction.

Claim 20 (previously presented): The computer system of claim 19, wherein the secondary device is a backing store.

Claim 21 (previously presented): The computer system of claim 19, wherein the secondary device is a swap device.

Claim 22 (previously presented): The computer system of claim 19, wherein the secondary device comprises an interface port comprising a socket connection.

Claim 23 (previously presented): The computer system of claim 22, wherein the socket connection comprises a computer network.

Claim 24 (previously presented): The computer system of claim 23, wherein the computer network comprises the Internet.

Claim 25 (currently amended): The computer system of claim 17, wherein the encryption key management system is further configured to encrypt ~~[[the]]~~ a pathname to the encrypted data file, the encryption key management system further configured to decrypt the pathname to the encrypted data file when retrieving encrypted data file contents.

Claim 26 (currently amended): A computer system comprising:

- a. a first device having an operating system kernel and a directory structure with directory information comprising encrypted data file names and corresponding encrypted data file locations for accessing encrypted data files within a file system, the operating system kernel configured to ~~encrypt clear data~~ decrypt the encrypted data file names and encrypted data file locations using ~~[[an]]~~ one or more encryption [[key]] keys to generate cipher ~~recover clear data corresponding to the data file names, data file locations, and data files,~~ the first device operating system kernel further configured to decrypt encrypt the cipher clear data using the one or more encryption [[key]] keys to generate the clear cipher data corresponding to the directory information and encrypted data files, ~~wherein the directory structure and corresponding directory information are encrypted;~~ and
- b. a second device coupled to the first device and configured to exchange cipher data with the first device.

Claim 27 (currently amended): The computer system of claim 26, wherein the operating system kernel is configured to encrypt ~~[[the]]~~ clear data and decrypt ~~[[the]]~~ cipher data using a symmetric algorithm.

Claim 28 (original): The computer system of claim 27, wherein the symmetric algorithm comprises a block cipher.

Claim 29 (original): The computer system of claim 28, wherein the block cipher comprises a Rijndael algorithm.

Claim 30 (currently amended): The computer system of claim 29, wherein one of the one or more encryption ~~[[key]]~~ keys comprises at least 1024 bits.

Claim 31 (original): The computer system of claim 26, wherein the second device comprises a backing store.

Claim 32 (original): The computer system of claim 26, wherein the second device comprises a swap device.

Claim 33 (previously presented): The computer system of claim 26, wherein the second device forms part of a communications channel.

Claim 34 (original): The computer system of claim 33, wherein the communications channel comprises a network.

Claim 35 (original): The computer system of claim 34, wherein the network comprises the Internet.

Claim 36 (currently amended): A method of ~~encrypting~~ storing an encrypted data file in a computer file system having a directory, the method comprising:

- a. receiving a clear data file having a name; and
- b. executing kernel code in an operating system, the kernel code configured to encrypt the clear data file to generate an encrypted data file using a symmetric key, store the encrypted data file at a location in the computer file system, and store in the directory an entry containing an encryption of the name and an encryption of the location ~~access data using an encrypted directory and using a symmetric key to encrypt the clear data to generate cipher data, the kernel code further using the symmetric key to decrypt the cipher data to generate the clear data.~~

Claim 37 (currently amended): The method of claim 36, wherein the symmetric key encrypts ~~[[the]]~~ clear data to generate cipher data according to a block cipher.

Claim 38 (original): The method of claim 37, wherein the block cipher comprises a Rijndael algorithm.

Claim 39 (original): The method of claim 37, wherein the block cipher comprises an algorithm selected from the group consisting of DES, triple-DES, Blowfish, and IDEA.

Claim 40 (currently amended): The method of claim 36, wherein executing kernel code comprises:

entering a pass key and a data file name into a first encryption process to produce an encrypted data file name and an encrypted data file name key; and
processing the file contents with the ~~encrypting~~ encrypted data file name key to generate an encrypted file contents key and an encrypted file contents.

Claim 41 (currently amended): The method of claim 40, further comprising:

storing the encrypted data file name key and the encrypted file contents key in a first protected area of a computer storage; and
storing the encrypted data file name and the encrypted file contents in a second protected area of the computer storage.

Claim 42 (currently amended): The method of claim 36, wherein executing kernel code to encrypt the clear data file ~~and decrypt cipher data~~ is performed when data is transferred between a computer memory and a secondary device.

Claim 43 (original): The method of claim 42, wherein the secondary device comprises a backing store.

Claim 44 (original): The method of claim 42, wherein the secondary device comprises a swap device.

Claim 45 (previously presented): The method of claim 42, wherein the secondary device forms part of a network of devices.

Claim 46 (canceled).

Claim 47 (previously presented): The method of claim 45, wherein the network comprises the Internet.

Claim 48 (currently amended): A computer system comprising:

- a. a processor;
- b. a physical memory ~~including an encrypted~~ containing an encrypted data file and a directory, and corresponding directory information for accessing data files wherein the directory comprises a record having a first element corresponding to an encrypted name of the data file and a second element corresponding to an encrypted location of the data file in the memory;
- c. a secondary device coupled to the physical memory; and
- d. an operating system comprising a kernel, the kernel configured to ~~access the data files using the encrypted directory and to encrypt and decrypt the encrypted data files transferred between the physical memory and the secondary device~~ decrypt the first and second elements to access the encrypted data file from memory when transferring the data file from the memory to the secondary device and to re-encrypt the first and second elements when transferring the data file from the secondary device to the memory.

Claim 49 (original): The computer system of claim 48, wherein the kernel is configured to encrypt and decrypt data using a symmetric key encryption algorithm.

Claim 50 (original): The computer system of claim 49, wherein the symmetric key encryption algorithm is based on a block cipher.

Claim 51 (previously presented): The computer system of claim 50, wherein the symmetric key encryption algorithm comprises Rijndael algorithm.

Claim 52 (original): The computer system of claim 51, wherein the kernel comprises a UNIX operating system.

Claims 53-58 (canceled)

Claim 59 (currently amended): The computer system of claim 1, further comprising:
one of encrypting and decrypting a data file in the directory with a corresponding file encryption key; and
one of encrypting and decrypting the directory with a directory encryption key.

Claim 60 (previously presented): The computer system of claim 59, wherein the corresponding file encryption keys are different.

Claim 61 (previously presented): The computer system of claim 1, wherein the encrypted directory comprises encrypted directory information including file names and locations of data blocks.

Claim 62 (currently amended): The computer system of claim 1, wherein the encrypted directory comprises encrypted directory information including data file names and corresponding i-node [[entry]] entries.

Claim 63 (previously presented): The computer system of claim 26, wherein the operating system kernel is further configured to locate a target directory by comparing an encrypted name of the target directory with encrypted names of candidate directories on the computer system.

Claim 64 (currently amended): The computer system of claim 26, wherein the directory information comprises data file names and locations of data blocks.

Claim 65 (currently amended): The computer system of claim 26, wherein the directory information comprises data file names and corresponding i-node [[entry]] entries.

Claim 66 (currently amended): The method of claim 36, wherein the **encrypted** directory comprises encrypted directory information including data file names and locations of data blocks.

Claim 67 (currently amended): The method of claim 36, wherein the **encrypted** directory comprises encrypted directory information including data file names and corresponding i-node [[entry]] entries.

Claim 68 (currently amended): The computer system of claim 48, wherein the directory ~~information~~ comprises data file names and locations of data blocks.

Claim 69 (currently amended): The computer system of claim 48, wherein the directory ~~information~~ comprises data file names and corresponding i-node [[entry]] entries.

Claim 70 (previously presented): A computer system containing an operating system, the computer system comprising:

- a kernel configured to encrypt and decrypt data transferred between a memory and a secondary device, wherein the kernel comprises an encryption engine configured to encrypt clear data to generate cipher data, the encryption engine further configured to decrypt the cipher data to generate the clear data;
- a memory coupled to the encryption engine and configured to store the cipher data, wherein the memory comprises a first logical protected memory configured to store encrypted file data and a second logical protected memory configured to store encrypted key data;
- an encryption key management system configured to control access to the encrypted file data and the encrypted key data, wherein the encryption key management system comprises a key engine, the key engine configured to receive a pass key and the file name to generate an encrypted file name key, use the encrypted file name key and file contents to generate an encrypted file contents key, and encrypt the file contents with the encrypted file contents key to generate encrypted file contents.

Claim 71 (previously presented): A method of encrypting data, the method comprising:

- receiving clear data; and
- executing kernel code in an operating system, wherein the kernel code is configured to use a symmetric key to encrypt the clear data to generate cipher data and to use the symmetric key to decrypt the cipher data to generate the clear data, and further wherein executing the kernel code comprises entering a pass key and a file name into a first encryption process to produce an encrypted file name and an encrypted file name key and processing the file contents with the encrypting file name key to generate an encrypted file contents key and encrypted file contents.